INTERNATIONALE STABILITÄT UND DIE SICHERHEIT DIGITALER PRODUKTE: DER «GENFER DIALOG»

Von Nele Achten

Cybersicherheit ist eine geteilte Verantwortung von Staat und Wirtschaft. Diese Erkenntnis ist nicht neu. Dennoch ist der internationale Dialog im Rahmen der Vereinten Nationen und anderen Fora zu Themen der Cybersicherheit häufig begrenzt auf staatliche Verantwortungen. Das internationale Recht war viele Jahre lang der Ausgangspunkt der Diskussionen. Somit ging es ausschliesslich um die Verantwortung von Staaten im Bereich der Informations- und Kommunikationstechnologien (ICT).[1] Der sogenannte «Genfer Dialog» verfolgt dagegen einen breiteren Ansatz: Private Unternehmen werden hier in die Themen der globalen Cybersicherheits- und Cyberaussenpolitik eingebunden.

Der «Genfer Dialog für verantwortungsvolles Verhalten im Cyberraum» wurde 2018 durch das Schweizer Eidgenössische Department für auswärtige Angelegenheiten (EDA) ins Leben gerufen. Das Center for Security Studies (CSS) unterstützt das EDA bei diesem Vorhaben von Beginn an und leistet inhaltliche Beiträge[2]. Mittlerweile hat sich die Dialogplattform weiterentwickelt und teilweise neu ausgerichtet. Die Flexibilität des Genfer Dialogs, sich an neue Entwicklungen auf internationaler Ebene anzupassen und den Ambitionen der unterschiedlichen Interessengruppen gerecht zu werden, ist seine Stärke. Es ist jedoch zugleich eine Herausforderung.

Phase I: Positionierung gegenüber existierenden parallelen Initiativen

Der Genfer Dialog wurde 2018 gegründet, nachdem die *UN Group of Governmental Experts* (UNGGE) 2016/17 daran gescheitert war, einen

1 Um die Verantwortung privater Unternehmen ging es nur indirekt, wenn es um die staatliche Verantwortung ging diese Akteure zu regulieren.

2 Siehe zum Beispiel eine Hintergrundrecherche zum Privatsektor: Jacqueline Eggenschwiler, *Geneva Dialogue on Responsible Behaviour in Cyberspace: Private Sector,* Framework Document (Zürich: ETH Zürich, 2018); für weitere Einzelheiten siehe auch: Jacqueline Eggenschwiler, «Geneva Dialogue: Mitgestaltung Globaler Sicherheitsnormen für den Cyberraum», in: Christian Nünlist / Oliver Thränert (Hrsg.), *Bulletin zur Schweizerischen Sicherheitspolitik* (Zürich: CSS, 2018), S. 119–22.

einstimmigen Abschlussbericht zu veröffentlichen. Die Gruppe von ExpertInnen studierte seit 2004 auf der Grundlage von unterschiedlichen, aufeinanderfolgenden Mandaten der UNO-Generalversammlung die Gefahren für die internationale Sicherheit, die durch die Nutzung von ICTs entstehen, und wie diese Gefahren adressiert werden sollten. Im einstimmigen Abschlussbericht der Gruppe 2014/15, der anschliessend durch die UNO-Generalversammlung bestätigt wurde, bekräftigten die Staaten die Anwendung des internationalen Rechts im Cyberraum und einigten sich auf dreizehn unverbindliche Normen des verantwortungsvollen Verhaltens von Staaten.

Etwa zum gleichen Zeitpunkt wie die Gründung des Genfer Dialogs entstanden auch einige normative Initiativen und Leitlinien des privaten Sektors, wie zum Beispiel die sogenannte *Charter of Trust for a Secure Digital World*[3] und der *Cybersecurity Tech Accord*[4]. Nachdem lange Zeit die staatliche Verantwortung und legale Antworten im Mittelpunkt standen, gewannen nun andere Themen an Bedeutung, insbesondere die Prävention von Cybersicherheitsvorfällen mit massiver Tragweite und die Frage, welche Verantwortung private Unternehmen hierbei zu tragen haben.

Seit Anfang 2017 stand zudem die von Microsoft initiierte Idee einer *Digital Geneva Convention* im Raum. Die Schweizer Regierung war ebenso wie viele andere westliche Staaten der Meinung, dass ein neues internationales Abkommen über die Verpflichtungen von Staaten im Cyberraum nicht erforderlich sei. Zugleich bestand Interesse, die Verantwortung des privaten Sektors in Themen der internationalen Cybersicherheitspolitik besser zu definieren. Somit ist es nicht überraschend, dass ein Austausch mit Unternehmen als vorläufiger Schwerpunkt des Genfer Dialogs identifiziert wurde.[5] Gleichzeitig hatte der Dialog zwischen Staaten bei den Vereinten Nationen zu diesem Zeitpunkt mit zwei

3 Siehe die Webseite der *Charter of Trust,* ursprünglich initiiert von Siemens und gegründet auf der Münchener Sicherheitskonferenz im Februar 2018.

4 Siehe die Webseite des *Cyber Tech Accord,* eine Initiative von Microsoft vom April 2018.

5 Paul Cornish / Camino Kavanagh, *Geneva Dialogue on Responsible Behaviour in Cyberspace: Phase 1 Report,* Mai 2019.

parallelen Arbeitsgruppen (OEWG und neue UNGGE[6]) bereits wieder neu an Fahrt aufgenommen.

Phase II: Dialog mit privaten Unternehmen zum Thema Sicherheit digitaler Produkte

Seit Anfang 2020 ist der Genfer Dialog eine Plattform des Austausches zwischen Vertreterinnen und Vertretern aus der Wirtschaft und aus staatlichen Institutionen. Die bisher rund dreissig Treffen wurden in Kooperation zwischen der DiploFoundation und dem EDA organisiert. Sie fanden aufgrund der COVID-19-Pandemie ausschliesslich online statt (der Track-1-Teil des Dialogs). Aufgrund dieses Formats konnten Unternehmensvertreterinnen und -vertreter von unterschiedlichen Kontinenten am Dialog teilnehmen. Die Regelmässigkeit der Treffen in jeder zweiten Woche trug zudem dazu bei, dass der Dialog inzwischen von einer vertrauensvollen und offenen Atmosphäre geprägt ist.

Inhaltlich liegt der Schwerpunkt des Dialoges auf der Sicherheit «digitaler Produkte». Dieser Begriff ist weit zu verstehen. Er beinhaltet unter anderem die Sicherheit von Software, dem *Internet of Things,* Cloud-Dienstleistungen und 5G-Technologien. Die Diskussionen über *best practices* wurden in einem Bericht Ende 2020 zusammengefasst.[7] Demnach ging es in den Gesprächen vor allen Dingen darum, das Verständnis und die Kernkomponenten von «sicherem Design» *(security by design)* digitaler Produkte besser nachzuvollziehen und zu definieren. Als Kernkomponenten wurden beispielsweise die Modellierung von Bedrohungen, die Sicherheit der von Drittherstellern integrierten Produkte *(supply chain security)* und Prozesse im Schwachstellenmanagement *(vulnerability processes)* identifiziert und diskutiert.

Im Jahr 2021 fanden zudem drei halbtägige Konferenzen statt zu den Themen «Sicherheit digitaler Produkte und Standardisierung» (Mai), «Regulierung der Sicherheit digitaler Produkte» (September)

6 Die *Open-ended Working Group,* deren Mandat hier einzusehen ist, und die *UN Group of Governmental Experts,* deren Mandat hier zu finden ist; beide wurden im Herbst 2018 neu initiiert.

7 Vladimir Radunović / Jonas Grätz, «Security of digital products and services: Reducing vulnerabilities and secure design – Industry good practices», *Geneva Dialogue,* Dezember 2020).

und «Globale Normen zur Sicherheit digitaler Produkte» (Dezember). Der Teilnehmerkreis dieser Veranstaltungen wurde erweitert und beinhaltete Vertreterinnen und Vertreter von Standardisierungsorganisationen, staatliche Entsandte nationaler Behörden der Cybersicherheit, DiplomatInnen, VertreterInnen aus der privaten Wirtschaft und Wissenschaft (der Track-2-Teil des Genfer Dialogs). Das CSS veröffentlichte einen Input-Bericht zur Regulierung und stellte ihn anlässlich der Konferenz im September vor. Zudem nahmen Vertreterinnen und Vertreter des CSS an allen Veranstaltungen des Track 1 und 2 teil.

Potenzial für die Zukunft und Herausforderungen

Eine Plattform für einen vertrauensvollen Austausch zwischen staatlichen und privaten Akteuren zu schaffen ist an sich bereits wertvoll. Dies ist umso bedeutsamer, als dieser Dialog in einem geopolitisch angespannten Umfeld gelang. Zudem nehmen am Genfer Dialog Unternehmen teil, die ihren Hauptsitz in den unterschiedlichen Grossmächten der Welt haben (insbesondere in China, Russland und den USA). In diesem Zusammenhang ist der Standort Genf sicherlich von Vorteil. Die Schweiz kann und sollte ihre Rolle als Vermittler für internationale Übereinkommen im Bereich der Sicherheit digitaler Produkte nutzen und weiter ausbauen.

Der Genfer Dialog hat zumindest bis 2024 eine strategische Basis in der Schweizer Aussenpolitik. Er ist in mehreren Strategien des Bundesrats genannt, insbesondere der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (2018–2022), der Aussenpolitischen Strategie (2020–2023), der Strategie Digitalaussenpolitik (2021–2024) und der China-Strategie (2021–2024). Es besteht der Anspruch, ein möglichst konkretes Ergebnis zu erzielen. Wie ein solch konkretes Ergebnis aussehen könnte, ist indes noch nicht klar.

Zu den offenen Fragen gehört beispielsweise: 1) Sollte das konkrete Ergebnis in Form von internationalen Richtlinien und einer Überprüfung durch eine internationale Organisation erfolgen? 2) Ist es notwendig, die Diskussion über die Sicherheit digitaler Produkte in unterschiedliche Technologien aufzugliedern. Während der Begriff des digitalen Produktes in zahlreichen internationalen Dokumenten und Strategien verwendet wird, wird auf der Implementierungsebene häufig

zwischen der Art des Produktes differenziert.[8] 3) Letztlich stellt sich die Frage, wer der Adressat der potenziellen Prinzipien oder Normen sein sollte? Wer sollte an der Ausarbeitung beteiligt sein? Und, wer sollte die tatsächliche Umsetzung kontrollieren?

8 So beinhaltet die Sicherheit von *Internet-of-Things*-Produkten und die Sicherheit der Cloud beispielsweise andere minimale Sicherheitsanforderungen, und Anreize zur Erhöhung der Sicherheit sollen auf unterschiedlichen regulatorischen Wegen geschaffen werden.